Customer Awareness

5 WAYS TO AVOID A PHISHING ATTACK

A **phishing attack** is a fake email designed by malicious hackers and thieves to look like it's coming from a trusted brand or institution–including your employer. The goal is to get you to click on the links and/or open an attachment.

Once you lower your guard and give up your personal information, financial data, or account logins, this information can be used to breach your employer's systems or compromise your identity.

The best way to defend yourself against phishing attacks is to **identify them before you can become a victim**.

Phishing is the act of obtaining information by pretending to be a legitimate source. Phishing could occur in two ways:

a) You reply to an email that asks for your personal or secretive information
b)You open an attachment or a link provided in an email

The following is a list of information you should pay attention to before giving out:

ID number
Bank account number
Full Name Company you work for
Credit card number
Credit limit
The number of cards you have
Information about the last transaction you made

Protect

*Update your computer on regular basis

*Update your browser and the browser's plug-ins regularly.

*Install the necessary software to protect your device, such as firewall, spam filters, anti-virus and anti-spyware, and ensure that they are updated regularly.

*Never type secretive (e.g. passwords or PIN) or personal information (e.g. name, location or salary) on shared or public devices.

*Check your transactions regularly. If you see any unusual transaction that you have not made, contact your bank immediately.

*Change your email or your online banking account passwords regularly.

*Do not reply emails with personal information.

Detect

Avoid responding to an email that:

a) Contains jargons, poor grammar or spelling mistakes.
b) Asks for your personal information.
c) Creates a sense of urgency.
d) Is not signed with the bank's logo or contact information.

*Never respond to calls or emails that ask for secret information such as PIN or passwords.

*Never respond to calls or emails that ask for personal or banking information e.g. credit card number, bank account number, id, name or phone number.

*Verify the identity of a caller before giving out any of your personal information, and directly call the call center.

*Do not open email attachments unless you expect and trust them.

*Avoid opening URLs and attachments that you receive by email, unless you expect them (e.g. password resetting URLs).

*If you would like to visit your bank's website, type the address on the browser yourself.

React

*Inform your bank immediately about any suspicious email or phone call that asks for our banking information.

*Contact your bank immediately if you believe that you have given your financial information while answering a phone call or an email.

*Change your email or online banking account passwords immediately if you suspect that your passwords might have been compromised.

*Contact your bank immediately, if you receive a transaction message from your bank that you do not recognize.

Ref: Banking Awareness tips by the financial sector information risk committee.